渗透测试概念

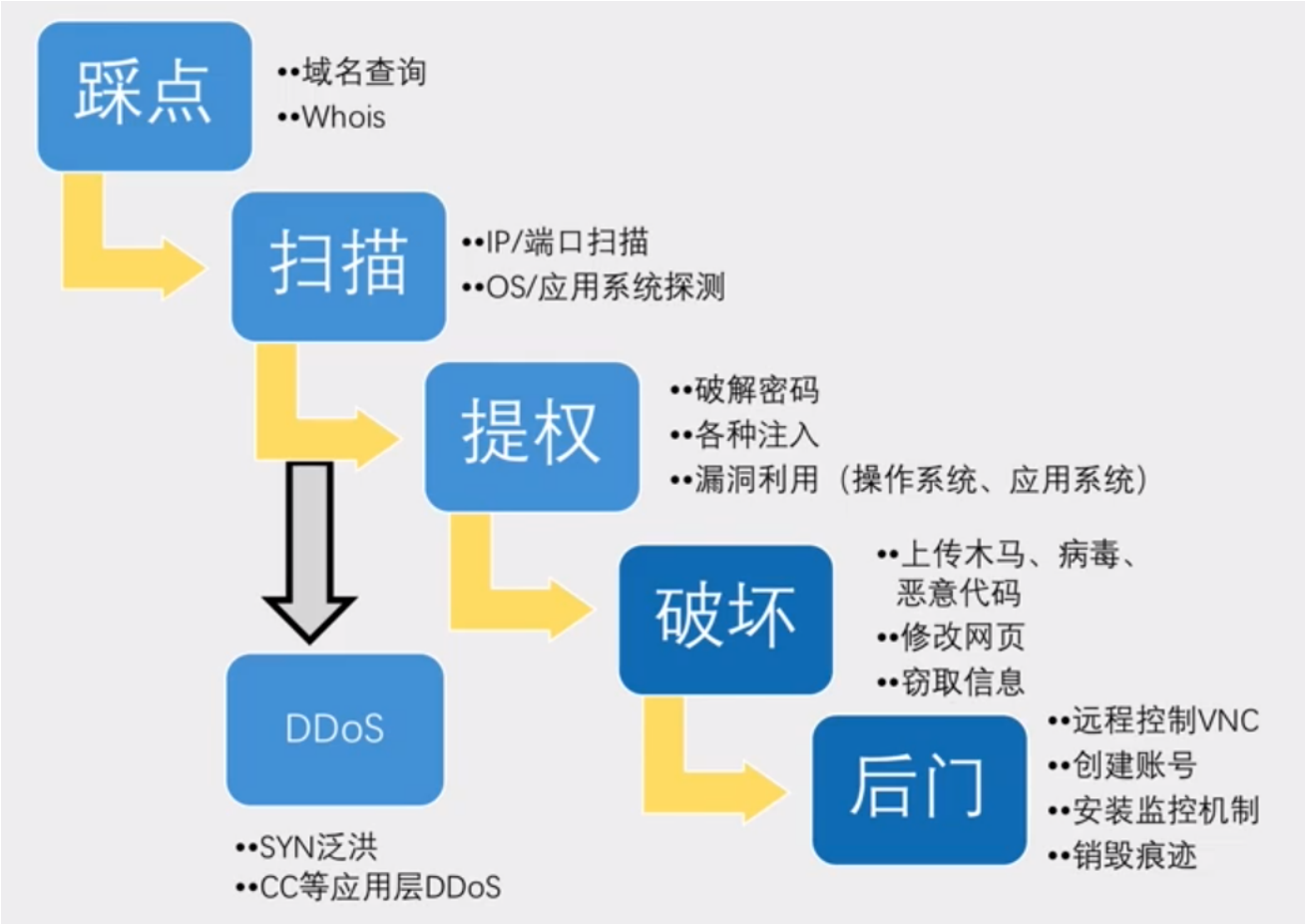
渗透测试就是利用我们所掌握的渗透知识，对网站进行一步一步的渗透，发现其中存在的漏洞和隐藏的风险，然后撰写一篇测试报告，提供给我们的客户。客户根据我们撰写的测试报告，对网站进行漏洞修补，以防止黑客的入侵！

渗透测试的前提是我们得经过用户的授权，才可以对网站进行渗透。如果我们没有经过客户的授权而对一个网站进行渗透测试的话，这是违法的。

渗透测试分为 **白盒测试** 和 **黑盒测试**

- 白盒测试就是在知道目标网站源码和其他一些信息的情况下对其进行渗透，有点类似于代码分析
- 黑盒测试就是只告诉我们这个网站的url，其他什么都不告诉，然后让你去渗透，模拟黑客对网站的渗透

渗透测试流程



信息收集概述（攻击前期）

信息收集对于渗透测试前期来说是非常重要的，因为只有我们掌握了目标网站或目标主机足够多的信息之后，我们才能更好地对其进行漏洞检测。正所谓，知己知彼百战百胜！

信息收集的方式可以分为两种：主动和被动。

主动信息收集：通过直接访问、扫描网站，这种流量将流经网站

被动信息收集：利用第三方的服务对目标进行访问了解，比例：Google搜索、Shodan搜索等

主动信息（网络扫描）

被动信息（网络踩点）

网络踩点概述

踩点信息

- 目标组织
  - 具体使用的域名
  - 网络地址范围
  - 因特网上可直接访问的IP地址与网络服务
  - 网络拓扑结构
  - 电话号码段
  - 电子邮件列表
  - 信息安全状况
- 目标个人
  - 身份信息、联系方式、职业经历，甚至一些个人隐私信息

踩点技术

- DNS与IP查询
  - 公开的一些因特网基础信息服务
  - 目标组织域名、IP以及地理位置之间的映射关系，以及注册的详细信息
- Web信息搜索与挖掘
  - “Google Hacking”
  - 对目标组织和个人的大量公开或意外泄漏的Web信息进行挖掘
- 网络拓扑侦察
  - 网络的网络拓扑结构和可能存在的网络访问路径

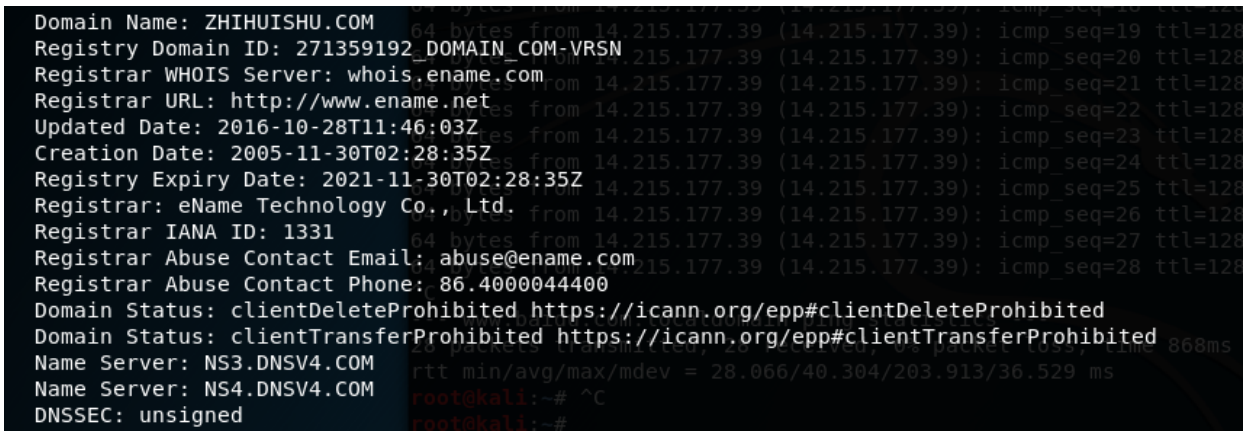
域名查询

whois域名注册信息查询

用来查询域名注册信息库的工具，一般的域名注册信息保护域名所有者、服务商、管理员邮件地址、域名注册日期和过期日期等等。

命令

```
whois testfire.net
whois zhihu.com
whois lucashu.cn
```



网站查询

http://tool.chinaz.com/

https://site.ip138.com/lucashu.cn/

IP查询

nslookup

```
nslookup baidu.com
```

dig

```
dig 8.8.8.8 baidu.com
```

补充

基于IP反查域名

http://stool.chinaz.com/

可以查询哪些域名指向同一个IP地址

http://stool.chinaz.com/same?s=210.42.176.9&page=

基于ip反查地址

https://www.maxmind.com/

搜索引擎搜集信息

Google Hacking

GoogleHacking：利用搜索引擎有争对性的搜索信息来对网络入侵的技术和行为。搜索引擎对于搜索的关键字提供了很多种语法，构造出特殊的关键字，能够快速全面的让攻击者挖掘到有价值的信息。

轻量级的搜索可搜索出一些遗留后门，不想被发现的后台入口，中量级的搜索出一些用户信息泄露，源代码泄露，未授权访问等等，重量级的则可能是mdb文件下载，CMS 未被锁定install页面，网站配置密码，php远程文件包含漏洞等重要信息。

基本用法

- 逻辑或： OR

  A OR B　　A + B　　系统查找含有检索词A、B之一，或同时包括检索词A和检索词B的信息。两者皆有，都会成为搜索结果

- 逻辑与：and

A AND B　　A*B　　可用来表示其所连接的两个检索项的交叉部分，也即交集部分。如果用AND连接检索词A和检索词B，则检索式为：A AND B(或A*B)：表示让系统检索同时包含检索词A和检索词B的信息集合C。

- 逻辑非： -

not keyword　-keyword　　强制结果不要出现此关键字

- 完整匹配："关键词"

"keyword"	强制搜索结果出现此关键字

高级用法

site

site:网址
功能：搜索指定的域名的网页内容 、可以用来搜索子域名、跟此域名相关的内容

site:pan.baidu.com “教程”

---

filetype

```
filetype:pdf                功能：搜索指定文件类型

"算法分析" filetype:pdf
site:csdn.net filetype:pdf
```

```
site:xx.com filetype:asp
site:xx.com filetype:php
site:xx.com filetype:jsp
site:xx.com filetype:aspx

site:hnucm.edu.cn filetype:php
```

---

inurl

```
inurl:keyword            功能：搜索url网址存在特定关键字的网页、可以用来搜寻有注入点的网站
```

```
inurl:.php?id=                                  搜索网址中有"php?id"的网页
inurl:.jsp?id=                                    搜索网址中有"jsp?id"的网页
inurl:.asp?id=                                     搜索网址中有"asp?id"的网页

inurl: /admin/login.php                  搜索网址中有"/admin/login.php"的网页

inurl:login       inurl:admin                                    搜索网址中有"login"等登录网页
inurl:config.txt
```

---

intitle

```
intitle:keyword 功能：搜索标题存在特定关键字的网页
```

```
intitle:后台登录

intitle:后台管理 filetype:php                  搜索网页标题是“后台管理”的php页面

intitle:index of "keyword"                       搜索此关键字相关的索引目录信息

intitle:index of "parent directory"          搜索根目录相关的索引目录信息
```

```
intitle:index of "password"                    搜索密码相关的索引目录信息
https://wikileaks.org/sony/docs/bonus/1/Password/50%20new%20user%20password.txt


intitle:index of "login"                              搜索登录页面信息

intitle:index of "admin"                            搜索后台管理页面信息
```

```
intitle:"Struts Problem Report"

intitle:"Struts Problem Report" intext:"development mode is enabled."
```

---

intext

```
intext:keyword          功能 ： 搜索正文存在特定关键字的网页
```

```
intext:Powered by Discuz                        搜索Discuz论坛相关的页面

intext:powered by wordpress                搜索wordpress制作的博客网址

intext:Powered by *CMS                          搜索CMS相关的页面

intext:powered by xxx inurl:login               搜索此类网址的后台登录页面
```

Google Hacking DataBase

https://www.exploit-db.com/google-hacking-database

Zoomeye Hacking && Shodan Hacking

> 首先，Shodan 是一个搜索引擎，但它与 Google 这种搜索网址的搜索引擎不同，Shodan 是用来搜索网络空间中在线设备的，你可以通过 Shodan 搜索指定的设备，或者搜索特定类型的设备，其中 Shodan 上最受欢迎的搜索内容是：webcam，linksys，cisco，netgear，SCADA等等。
>
> 那么 Shodan 是怎么工作的呢？Shodan 通过扫描全网设备并抓取解析各个设备返回的 banner 信息，通过了解这些信息 Shodan 就能得知网络中哪一种 Web 服务器是最受欢迎的，或是网络中到底存在多少可匿名登录的 FTP 服务器。或者哪个ip对应的主机是哪种设备。
>
> 可扫描一切联网的设备，除了常见的Web服务器，还能扫描防火墙、路由器、交换机、摄像头、打印机等一切联网设备

官网：http://zoomeye.org/ 钟馗之眼

官网：https://www.shodan.io/

帮助文档：https://www.zoomeye.org/doc?channel=user

探索： https://www.zoomeye.org/statistics

zoomeye 快捷键

- `Shift/` 显示帮助键
- `Esc` 隐藏帮助键
- `Shift h` 回到首页
- `Shift s` 高级搜索
- `s` 聚集搜索框

搜索组件名称

```
app: 组件名

ver: 组件版本

Apache httpd, 版本2.2.16: app:"Apache httpd" +ver:"2.2.16"
```

搜索端口

```
port：开放端口                常用端口号

搜索远程桌面连接: port:3389

搜索SSH: port:22

mstsc -v
```

搜索操作系统

```
os: 操作系统                    os:linux
```

搜索主机名和ip

```
hostname: 分析列表中的"主机名"字段。例子: hostname:baidu.com

ip: 搜索一个指定的IP地址。ip:8.8.8.8

site: 网站域名  site:google.com
```

搜索网站

```
title: 页面标题，在<title>例子: title:Nginx

关键字   keywords: 定义的页面关键字。 例子: keywords:Nginx

描述     keywords: 定义的页面说明。 例子: desc:Nginx

HTTP头  headers: HTPP请求中的Headers。例子: headers:Server
```

搜索组件

```
搜索组件:  https://www.zoomeye.org/component
```